CLAIMS

1. A system for processing a computer file to determine whether it contains a virus or other malware comprising:

a) means for generating data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file;

b) means for selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware; and

c) means for determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe and for controlling the means b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the means b) at all.

2. A system according to claim 1 wherein the controlling means c) controls the means b) in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected.

3. A system according to claim 1 or 2 wherein the controlling means c) controls the means b) in dependence on factors including sources, recorded in the database, from which instances of the file have originated.

4. A system according to claim 1, 2 or 3 wherein the controlling means c) controls the means b) in dependence on factors including the number of times, recorded in the database, of instances of the file have been processed.

5. A system according to any one of the preceding claims, and including means for updating the database in dependence upon the result of the processing of the file by the means b).

6. A system according to claim 5 wherein the updating of the database, in the event of the means b) determining that the file contains, or is likely to contain, malware is such that the record thereof in the database is deleted, or updated so that it is no longer taken be safe.

7. A method of processing a computer file to determine whether it contains a virus or other malware comprising:

a) generating data with regard to the file to characterise its identity and for thereby referencing a computer database to determine whether it is an instance of a known file;

b) selectively subjecting the file to a number of heuristic procedures to determine whether or not it contains, or is likely to contain, malware; and

c) determining, in dependence upon the record, if any, of the file in the database, whether the file can be regarded as safe and conducting the step b) such that the file, if the file is to be regarded as safe, is either subject to less thorough processing than if it were not so regarded or not subject to processing by the step b) at all.

8. A method according to claim 7 wherein the determining step c) controls the step b) in dependence on factors including the length of time for which the database indicates that the file has been known without malware-containing instances of it being detected.

9. A method according to claim 7 or 8 wherein the determining step c) controls the step b) in dependence on factors including sources, recorded in the database, from which instances of the file have originated.

10. A method according to claim 7, 8 or 9 wherein the determining step c) controls the step b) in dependence on factors including the number of times, recorded in the database, instances of the file have been processed.

11. A method according to any one claims 7 to 10, and including the step of updating the database in dependence upon the result of the processing of the file by the step b).

12. A method according to claim 11 wherein the updating of the database, in the event of the step b) determining that the file contains, or is likely to contain, malware is such that the record thereof in the database is deleted, or updated so that it is no longer taken be safe.

13. A system for processing a computer file to determine whether it contains a virus or other malware substantially as hereinbefore described and with reference to the accompanying drawings

14. A method of processing a computer file to determine whether it contains a virus or other malware substantially as hereinbefore described and with reference to the accompanying drawings